PATENT ABSTRACTS OF JAPAN

(11)Publication number : 10-275114
(43)Date of publication of application : 13.10.1998

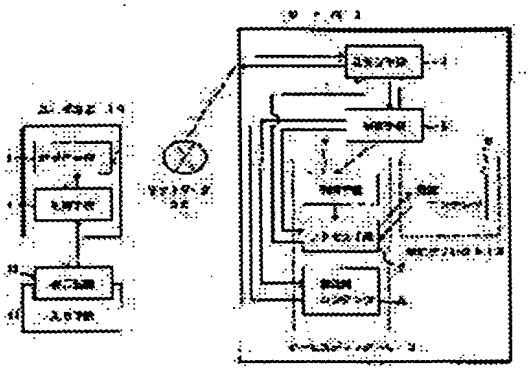
(51)Int.Cl. G06F 12/14
G06F 12/00
G06F 15/00

(21)Application number : 09-080909
(22)Date of filing : 31.03.1997

(71)Applicant : FUJITSU LTD
(72)Inventor : ISOYAMA TOMOHIRO
SHIBUE YUJI

(54) CONTENT SECURITY METHOD OF INTERNET AND SYSTEM THEREFOR

(57)Abstract:
PROBLEM TO BE SOLVED: To prevent a user who is not allowed to gain access to access limited contents by providing the limited contents in a directory other than service directories on a server and permitting a user who is allowed to gain access to access the limited contents.
SOLUTION: A parameter judging means 6 checks whether or not a user sent from a user terminal 10 is present and whether or not a password is correct according to data stored previously in a data base provided in the directory 3 other than the service directories 2 on the server 1. When it is judged that the user is permitted to access the limited contents B, an access means 7 accesses the initial HTML page (e.g. menu page) of the limited contents B set previously corresponding to parameters, sends the initial HTML page similarly to a password page, and displays it on a display device 13.



LEGAL STATUS

[Date of request for examination] 23.10.2003
[Date of sending the examiner's decision of rejection]
[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]
[Date of final disposal for application]
[Patent number]
[Date of registration]
[Number of appeal against examiner's decision of rejection]
[Date of requesting appeal against examiner's decision of rejection]
[Date of extinction of right]

CLAIMS

[Claim(s)]
[Claim 1] When a user prepares on a server the service directory which can be perused freely and gives a specific parameter from a user terminal In the contents security approach of the Internet that the access permission to the limited contents of the specified use corresponding to the above-mentioned parameter is given among the contents prepared in the above-mentioned service directory The above-mentioned limited contents are prepared in other directories other than the service directory on the above-mentioned server. The contents security approach of the Internet characterized by accessing the above-mentioned limited contents when it is judged that it is access [user / by whom the above-mentioned access permission was given].
[Claim 2] When a user prepares on a server the service directory which can be perused freely and gives a specific parameter from a user terminal In the contents security system of the Internet by which the access permission to the limited contents of the specified use corresponding to the above-mentioned parameter is given among the contents prepared in the above-mentioned service directory While being prepared in the above-mentioned limited contents with which other directories other than the service directory on the above-mentioned server were equipped, and the service directory on the above-mentioned server The contents security system of the Internet characterized by having an access means to access the above-mentioned limited contents when it is judged that it is access [user / by whom the above-mentioned access permission was given].

[Translation done.]

DETAILED DESCRIPTION

[Detailed Description of the Invention]
[0001]
[Industrial Application] This invention relates to the contents security approach and system of the Internet which are used in the Internet system.
[0002]
[Description of the Prior Art] Now, the Internet system by which many and unspecified users connected through the network stretched and plotted all over the world can peruse freely the contents created on the server spreads, and the service only for a specific user is also increasing in it. This service manages user ID, a password, etc., and when it is judged that he is the specific user by whom authorization of access was given with the password check, it enables it to peruse the limited contents created for the specific user. Hereafter, this conventional security system is explained based on drawing 4 .
[0003] On the server 31 used in the Internet system, the service directory 32 which can be freely perused through a network 34 from a user terminal 33 by the browser which is a browser is formed, and the release contents A by which release is carried out, the above-mentioned limited contents B, etc. are edited into this service directory 32.
[0004] When perusing the HTML page of the release contents A from the above-mentioned user terminal 33, it can access and peruse by choosing and performing the link which carried out the direct input of the URL which is the server address of the HTML page made into the object from the above-mentioned browser, and the address in a server, or was prepared in the HTML page under present access.
[0005] Moreover, when perusing the HTML page of the above-mentioned limited contents B from the above-mentioned user terminal 33, the HTML page (henceforth a password page) which enters user ID, a password, etc. like the case of the above-mentioned release contents A is displayed. Next, when user ID and a password were entered from this password page and it is judged based on the data of the database which it had beforehand on the server that whether the user ID inputted as mentioned above existing and a password are the users by whom the check of the right etc. was performed and the access permission to the above-mentioned limited contents B was given, these limited contents B can be accessed and it can peruse.
[0006] However, the contents generally edited into the above-mentioned service directory 32 on a server 31 can be accessed regardless of distinction of the release contents A, the limited contents B, etc. by carrying out the direct input of the URL of these contents on the above-mentioned browser. Therefore, with the above conventional security, when the above-mentioned password page establishes a link in the release contents A etc. or the limited contents B make URL of itself secret to carrying out [exhibit / direct URL], it has prevented being accessed by the above-mentioned limited contents B without passing through the above-mentioned password page.
[0007]
[Problem(s) to be Solved by the Invention] With the above conventional security, if known, the location, i.e., URL, of the above-mentioned limited contents B, even if it is the user by whom the access permission is not given, access to the above-mentioned limited contents B can be performed by carrying out the direct input of this URL on the above-mentioned browser.
[0008] Therefore, although URL of the above-mentioned limited contents B is made secret For example, when URL of release and the limited contents B is alike From URL of the release contents A, the user by whom the access permission is not given guesses URL of the above-mentioned limited contents B, and inputs, or Moreover, it may happen that will input URL of the above-mentioned limited contents B by chance, and URL of the above-mentioned limited contents B will be known or to use URL of the above-mentioned limited contents B which could be known before, after the user who had the access permission before loses rating.
[0009] With the conventional security, it was not able to prevent thoroughly being accessed by the user by whom the access permission is not given to the above-mentioned limited contents B as mentioned above.
[0010] This invention is proposed in view of the above-mentioned situation, only the user by whom the access permission to the above-mentioned limited contents was given can access it to these limited contents, and the user by whom the access permission is not given aims at offering the contents security approach and system of the Internet which can prevent accessing to these limited contents certainly.
[0011]
[Means for Solving the Problem] This invention has adopted the following means, in order to attain the above-mentioned object. Namely, when a user forms the service directory 2 which can be perused freely on a server 1 and gives a specific parameter from a user terminal 10 In the contents security approach of the Internet that the access permission to the limited contents B of the specified use corresponding to the above-mentioned parameter is given among the contents prepared in the above-mentioned service directory 2 The above-mentioned limited contents B were formed in other directories 3 other than service directory 2 on the above-mentioned server 1, and when it is judged that it is access [user / by whom the above-mentioned access permission was given], a means to access the above-mentioned limited contents B is adopted.
[0012] While specifically being prepared in the service directory 2 on the above-mentioned limited contents B with which other directories 3 other than service directory 2 on the above-mentioned server 1 were equipped, and the above-mentioned server 1, when it is judged that it is access [user / by whom the above-mentioned access permission was given], it realizes by having an access means to access the above-mentioned limited contents B.
[0013]
[Embodiment of the Invention] Drawing 1 is the conceptual diagram of the network where the contents security system of the

Internet of this invention is applied. drawing 2 is the block diagram of one example of the contents security system of the Internet of this invention, and drawing 3 is flow drawing showing the procedure in the above-mentioned system, and it explains it based on drawing below.

[0014] In this example, the release contents A which contain a password page in the service directory 2 on a server 1, the parameter decision means 6, and the access means 7 are formed for the limited contents B in other directories 3 other than service directory 2.

[0015] When perusing the above-mentioned limited contents B on the server 1 connected through the network 20 from the user terminal 10, the above-mentioned password page first prepared in the above-mentioned service directory 2 is displayed.

[whether this procedure inputs URL of the direct above-mentioned password page from on the browser started by the control means 11 of the above-mentioned user terminal with the input means 14, such as a keyboard of the above-mentioned user terminal 10, and a mouse, and] Or if the link of the above-mentioned password page prepared in the HTML page of the release contents A is chosen and performed (S1) URL of the above-mentioned password page is sent to the transceiver means 4 of the above-mentioned server 1 from this transceiver means 4 next through a network 20 from the transceiver means 12 of a user terminal 10 to a control means 5 based on the server address in this URL (S2). This control means 5 sends the above-mentioned password page to the above-mentioned transceiver means 12 of the above-mentioned user terminal 10 through the above-mentioned transceiver means 4 and a network 20 based on the address in a server in sent URL. Next, in the above-mentioned user terminal 10, the transmitted above-mentioned password page is displayed on the display 13 of the above-mentioned user terminal 10 by the above-mentioned browser (S3).

[0016] And next, if a user gives and enters user ID and a password into this password page as a parameter with the above-mentioned input means 14 (S4), it will be transmitted to the above-mentioned control means 5 through the transceiver means 4 of the above-mentioned network 20 and the above-mentioned server 1 from the above-mentioned transceiver means 12 like URL of the above-mentioned password page, and the parameter decision means 6 will be started by this control means 5. With this parameter decision means 6, the above-mentioned user ID transmitted to the database formed in other directories 3 other than the above-mentioned service directory 2 on a server 1 from the user terminal 10 based on the data stored beforehand exists, or the above-mentioned password is performing that check (S5) of the right.

[0017] Consequently, when it is judged that he is the user by whom the access permission to the above-mentioned limited contents B was given, it accesses to the initial HTML pages (for example, menu page shown in drawing 4) of the limited contents B to which the access means 7 was beforehand set corresponding to the above-mentioned parameter (S6), this initial HTML page is transmitted to the above-mentioned user terminal 10 like the above-mentioned password page, and it is made to display on the above-mentioned display 13 (S7). at least one display [degree] items 21 (for example, item of the HTML page which can be displayed on a degree on the menu page shown in drawing 4 etc.) hang up over this initial HTML page -- having -- **** -- a user -- this -- degree screen can be chosen now by directing either of degree display items 21. That is, the assignment of a purport of the display HTML name 22 of the full path which indicated the directory of the storing location of this following display item to each hiding in the above-mentioned following display item 21 from a user in the format (it not being displayed on a screen but stored in the memory of the above-mentioned user terminal 10 etc.) which is not in sight, and being given to it as a parameter, and adding to the display HTML name 22 of this full path, and starting the above-mentioned access means 7 is made. Degree screen corresponding to degree display item 21 of the specification chosen as mentioned above by this based on directions of a user can be displayed.

[0018] In addition, when it is judged as a result of the above-mentioned check that he is not the user by whom the access permission to the above-mentioned limited contents B was given, access to the above-mentioned initial HTML page is not performed, but the display of a purport without an access permission is made by the above-mentioned display 13 (S8).

[0019] next, the above which the user chose -- if degree display item 21 is performed (S9) -- this -- the display HTML name 22 of the full path of the display [degree] item 21 is transmitted to the above-mentioned control means 5 like URL of the above-mentioned password page as a parameter, and the above-mentioned access means 7 is started. Degree display chosen by the display HTML name 22 of the full path which is the transmitted parameter is accessed (S10), this following display is transmitted to a user terminal 10 like the above-mentioned password page, and it is expressed to the above-mentioned display 13 as this access means 7 (S11). access to degree display of the limited contents B after this -- the above -- it is carried out like the access method to degree display.

[0020] Moreover, by choosing and performing the link established in the screen under access in the above-mentioned limited contents B even if it was a user under utilization at which event with the above-mentioned input means 14, or inputting URL of the direct release contents A with the above-mentioned input means 14 from on the above-mentioned browser, access of the above-mentioned limited contents B can be ended, and it can move to access of the release contents A.

[0021]

[Effect of the Invention] According to the contents security approach and system of the Internet of this invention, access from the user by whom the access permission to these limited contents is not given can be certainly prevented by having prepared limited contents in other directories other than the service directory on a server, and having formed an access means to access the above-mentioned limited contents when it is judged that it is access [user / by whom the access permission was given] in the service directory on the above-mentioned server.

[Translation done.]

DESCRIPTION OF DRAWINGS

[Brief Description of the Drawings]
[Drawing 1] It is the conceptual diagram of the network where this invention is applied.
[Drawing 2] It is the block diagram of one example of this invention.
[Drawing 3] It is flow drawing of one example of this invention.
[Drawing 4] It is the example of a screen of one example of this invention.
[Drawing 5] It is the conventional system concept drawing.
[Description of Notations]
1 31 Server
2 32 Service Directory
3 Other Directories
4 12 Transceiver means
5 11 Control means
6 Parameter Decision Means
7 Access Means
10 33 User terminal
13 Display
20 34 Network
A Release contents
B Limited contents

[Translation done.]

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（A）　(11)特許出願公開番号

特開平10－275114

(43)公開日　平成10年(1998)10月13日

(51)Int.Cl.[6]		識別記号	FI		
G06F	12/14	310	C06F	12/14	310K
	12/00	537		12/00	537A
	15/00	330		15/00	330D

審査請求　未請求　請求項の数2　OL　（全 7 頁）

(21)出願番号　特願平9－80909

(22)出願日　平成９年(1997)３月31日

(71)出願人　000005223
富士通株式会社
神奈川県川崎市中原区上小田中４丁目１番１号

(72)発明者　磯山　朋宏
岡山県岡山市津島京町10番12号　株式会社富士通岡山システムエンジニアリング内

(72)発明者　渋江　裕司
岡山県岡山市津島京町10番12号　株式会社富士通岡山システムエンジニアリング内

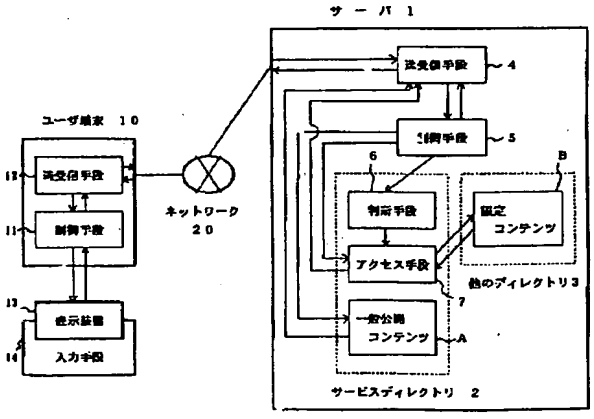
(74)代理人　弁理士　福井　豊明

(54)【発明の名称】　インターネットのコンテンツセキュリティ方法およびシステム

(57)【要約】

【課題】　インターネットのシステムにおいて利用されるインターネットのコンテンツセキュリティ方法およびシステムに関するものである。

【解決手段】　ユーザが自由に閲覧することができるサーバ上のサービスディレクトリ以外の他のディレクトリに特定用途の限定コンテンツを設け、ユーザ端末より特定のパラメータを与えることによって、上記限定コンテンツへのアクセス許可が与えられた場合に上記限定コンテンツをアクセスする。よって、上記限定コンテンツへのアクセス許可が与えられた者だけが該限定コンテンツへアクセスすることができ、アクセス許可が与えられていない者が該限定コンテンツへアクセスすることを確実に防止することのできる。



【特許請求の範囲】
【請求項１】　ユーザが自由に閲覧することができるサービスディレクトリをサーバ上に設け、ユーザ端末より特定のパラメータを与えることによって、上記サービスディレクトリに設けたコンテンツのうち上記パラメータに対応した特定用途の限定コンテンツへのアクセス許可が与えられるインターネットのコンテンツセキュリティ方法において、
上記限定コンテンツを上記サーバ上のサービスディレクトリ以外の他のディレクトリに設け、上記アクセス許可が与えられたユーザよりのアクセスであると判断した場合に、上記限定コンテンツをアクセスすることを特徴とするインターネットのコンテンツセキュリティ方法。
【請求項２】　ユーザが自由に閲覧することができるサービスディレクトリをサーバ上に設け、ユーザ端末より特定のパラメータを与えることによって、上記サービスディレクトリに設けたコンテンツのうち上記パラメータに対応した特定用途の限定コンテンツへのアクセス許可が与えられるインターネットのコンテンツセキュリティシステムにおいて、
上記サーバ上のサービスディレクトリ以外の他のディレクトリに備えた上記限定コンテンツと、
上記サーバ上のサービスディレクトリに設けられるとともに、上記アクセス許可が与えられたユーザよりのアクセスであると判断した場合に上記限定コンテンツをアクセスするアクセス手段とを備えたことを特徴とするインターネットのコンテンツセキュリティシステム。
【発明の詳細な説明】
【０００１】
【産業上の利用分野】本発明はインターネットシステムにおいて利用されるインターネットのコンテンツセキュリティ方法およびシステムに関するものである。
【０００２】
【従来技術】現在、世界中にはりめぐらされたネットワークを介して接続された不特定多数のユーザがサーバ上に作成されたコンテンツを自由に閲覧することができるインターネットシステムが普及し、その中で特定のユーザだけを対象としたサービスも増加している。このサービスは、ユーザＩＤ、パスワード等を管理し、パスワードチェックでアクセスの許可が与えられた特定のユーザであると判断された場合に、特定のユーザを対象にして作成された限定コンテンツを閲覧することができるようにしている。以下、この従来のセキュリティシステムについて図４に基づいて説明する。
【０００３】インターネットシステムにおいて利用されるサーバ３１上には閲覧ソフトであるブラウザによってユーザ端末３３からネットワーク３４を介して自由に閲覧することができるサービスディレクトリ３２が設けられており、該サービスディレクトリ３２に一般公開される一般公開コンテンツＡおよび上記限定コンテンツＢ等が編集されている。
【０００４】上記ユーザ端末３３より一般公開コンテンツＡのＨＴＭＬページを閲覧する場合、上記ブラウザより目的とするＨＴＭＬページのサーバアドレスおよびサーバ内アドレスであるＵＲＬを直接入力するか、または現在閲覧中のＨＴＭＬページ内に設けられたリンクを選択し実行することによってアクセスし閲覧することができる。
【０００５】また、上記ユーザ端末３３より上記限定コンテンツＢのＨＴＭＬページを閲覧する場合、上記一般公開コンテンツＡの場合と同様にしてユーザＩＤおよびパスワード等の入力を行うＨＴＭＬページ（以下、パスワードページと言う）を表示させる。次に該パスワードページよりユーザＩＤおよびパスワードを入力すると、サーバ上に予め備えられたデータベースのデータに基づいて、上記のように入力されたユーザＩＤは存在するか、またパスワードが正しいか等のチェックが行われ、上記限定コンテンツＢへのアクセス許可が与えられたユーザであると判断された場合に該限定コンテンツＢにアクセスし閲覧することができる。
【０００６】しかしながら、一般にサーバ３１上の上記サービスディレクトリ３２に編集されたコンテンツは一般公開コンテンツＡ、限定コンテンツＢ等の区別に関係なく、上記ブラウザ上でこれらコンテンツのＵＲＬを直接入力することでアクセスすることができる。したがって、上記のような従来のセキュリティでは、上記パスワードページは一般公開コンテンツＡ等にリンクを設けるか、または直接ＵＲＬを公開するなどしているのに対して、限定コンテンツＢはそれ自体のＵＲＬを非公開とすることによって、上記パスワードページを経ないで上記限定コンテンツＢにアクセスされることを防止している。
【０００７】
【発明が解決しようとする課題】上記のような従来のセキュリティでは、もし上記限定コンテンツＢの場所すなわちＵＲＬが知られれば、アクセス許可が与えられていないユーザであっても、上記ブラウザ上で該ＵＲＬを直接入力することで、上記限定コンテンツＢへのアクセスを行うことができることになる。
【０００８】よって上記限定コンテンツＢのＵＲＬは非公開とされているが、例えば一般公開および限定コンテンツＢのＵＲＬが似かよっている場合に、アクセス許可が与えられていないユーザが一般公開コンテンツＡのＵＲＬより上記限定コンテンツＢのＵＲＬを類推して入力したり、また偶然に上記限定コンテンツＢのＵＲＬを入力したりして上記限定コンテンツＢのＵＲＬが知られてしまうことや、以前アクセス許可を有していたユーザが資格を喪失した後に、以前に知り得た上記限定コンテンツＢのＵＲＬを利用することが起こりえる。
【０００９】以上のように従来のセキュリティでは、ア

クセス許可が与えられていないユーザによって上記限定コンテンツＢへアクセスされることを完全に防止することができなかった。

【００１０】本発明は上記の事情に鑑みて提案されたものであり、上記限定コンテンツへのアクセス許可が与えられたユーザだけが該限定コンテンツへアクセスすることができ、アクセス許可が与えられていないユーザが該限定コンテンツへアクセスすることを確実に防止することのできるインターネットのコンテンツセキュリティ方法およびシステムを提供することを目的とする。

【００１１】

【課題を解決するための手段】本発明は上記目的を達成するために以下の手段を採用している。すなわち、ユーザが自由に閲覧することができるサービスディレクトリ２をサーバ１上に設け、ユーザ端末１０より特定のパラメータを与えることによって、上記サービスディレクトリ２に設けたコンテンツのうち上記パラメータに対応した特定用途の限定コンテンツＢへのアクセス許可が与えられるインターネットのコンテンツセキュリティ方法において、上記限定コンテンツＢを上記サーバ１上のサービスディレクトリ２以外の他のディレクトリ３に設け、上記アクセス許可が与えられたユーザよりのアクセスであると判断した場合に、上記限定コンテンツＢをアクセスするという手段を採用している。

【００１２】具体的には、上記サーバ１上のサービスディレクトリ２以外の他のディレクトリ３に備えた上記限定コンテンツＢと、上記サーバ１上のサービスディレクトリ２に設けられるとともに、上記アクセス許可が与えられたユーザよりのアクセスであると判断した場合に上記限定コンテンツＢをアクセスするアクセス手段とを備えることによって実現する。

【００１３】

【実施の形態】図１は本発明のインターネットのコンテンツセキュリティシステムの適用されるネットワークの概念図であり、図２は本発明のインターネットのコンテンツセキュリティシステムの一実施例のブロック図であり、図３は上記システムにおける処理手順を示すフロー図であり、以下図に基づいて説明する。

【００１４】本実施例において、サーバ１上のサービスディレクトリ２にはパスワードページを含む一般公開コンテンツＡ、パラメータ判断手段６、アクセス手段７を、サービスディレクトリ２以外の他のディレクトリ３には限定コンテンツＢを設けている。

【００１５】ユーザ端末１０よりネットワーク２０を介して接続されたサーバ１上の上記限定コンテンツＢを閲覧する場合、まず最初に上記サービスディレクトリ２に設けた上記パスワードページを表示させる。この手順は、上記ユーザ端末１０のキーボードやマウス等の入力手段１４で上記ユーザ端末の制御手段１１により起動されたブラウザ上から直接上記パスワードページのＵＲＬを入力するか、または一般公開コンテンツＡのＨＴＭＬページ内に設けられた上記パスワードページのリンクを選択して実行（Ｓ１）すれば、上記パスワードページのＵＲＬがユーザ端末１０の送受信手段１２から、該ＵＲＬ中のサーバアドレスに基づいてネットワーク２０を介して上記サーバ１の送受信手段４へ、次に該送受信手段４より制御手段５へ送られる（Ｓ２）。該制御手段５は送られたＵＲＬ中のサーバ内アドレスに基づいて上記パスワードページを上記送受信手段４、ネットワーク２０を介して上記ユーザ端末１０の上記送受信手段１２へ送る。次に上記ユーザ端末１０では、送信されてきた上記パスワードページが上記ブラウザによって上記ユーザ端末１０の表示装置１３に表示される（Ｓ３）。

【００１６】そして次に、該パスワードページにユーザが上記入力手段１４によってパラメータとしてユーザＩＤおよびパスワードを与えて入力（Ｓ４）すれば、上記パスワードページのＵＲＬと同様にして上記送受信手段１２から上記ネットワーク２０、上記サーバ１の送受信手段４を介して上記制御手段５へ送信され、該制御手段５によりパラメータ判断手段６が起動される。該パラメータ判断手段６では、サーバ１上の上記サービスディレクトリ２以外の他のディレクトリ３に設けられたデータベースに予め蓄積されたデータに基づいてユーザ端末１０より送信されてきた上記ユーザＩＤが存在するか、また上記パスワードが正しいのかのチェック（Ｓ５）を行っている。

【００１７】その結果、上記限定コンテンツＢへのアクセス許可が与えられたユーザであると判断した場合、アクセス手段７が上記パラメータに対応して予め設定された限定コンテンツＢの初期ＨＴＭＬページ（例えば図４に示すメニューページ等）へアクセス（Ｓ６）を行い、該初期ＨＴＭＬページを上記パスワードページと同様にして上記ユーザ端末１０へ送信し、上記表示装置１３に表示（Ｓ７）させる。この初期ＨＴＭＬページには少なくとも１つの次表示項目２１（例えば図４に示すメニューページでは次に表示することのできるＨＴＭＬページの項目等）が掲げられており、ユーザが該次表示項目２１のいずれかを指示することによって、次画面を選択することができるようになっている。すなわち、上記次表示項目２１にはそれぞれに該次表示項目の格納場所のディレクトリを記載したフルパスの表示ＨＴＭＬ名２２がユーザには見えない形式（画面には表示されず上記ユーザ端末１０のメモリ等に格納される）で隠しパラメータとして付与されており、また該フルパスの表示ＨＴＭＬ名２２に追加して上記アクセス手段７を起動する旨の指定がなされている。これによって、上記のようにユーザの指示に基づいて選択された特定の次表示項目２１に対応した次画面を表示することができる。

【００１８】尚、上記チェックの結果、上記限定コンテンツＢへのアクセス許可が与えられたユーザでないと判

断した場合、上記初期ＨＴＭＬページへのアクセスは行われず、アクセス許可がない旨の表示が上記表示装置１３になされる（Ｓ８）。

【００１９】次に、ユーザが選択した上記次表示項目２１を実行（Ｓ９）すれば、該次表示項目２１のフルパスの表示ＨＴＭＬ名２２がパラメータとして上記パスワードページのＵＲＬと同様にして上記制御手段５に送信され上記アクセス手段７が起動される。該アクセス手段７では送信されたパラメータであるフルパスの表示ＨＴＭＬ名２２によって選択された次表示をアクセス（Ｓ１０）して、該次表示が上記パスワードページと同様にしてユーザ端末１０へ送信され、上記表示装置１３に表示（Ｓ１１）される。これ以降の限定コンテンツＢの次表示へのアクセスは、上記次表示へのアクセス手順と同様にして行われる。

【００２０】また、上記限定コンテンツＢを利用中のユーザは、どの時点であっても閲覧中の画面に設けられたリンクを上記入力手段１４で選択して実行するか、または上記ブラウザ上から直接一般公開コンテンツＡのＵＲＬを上記入力手段１４で入力することによって、上記限定コンテンツＢの閲覧を終了して一般公開コンテンツＡの閲覧に移ることができる。

【００２１】

【発明の効果】本発明のインターネットのコンテンツセキュリティ方法およびシステムによれば、限定コンテンツをサーバ上のサービスディレクトリ以外の他のディレクトリに設け、アクセス許可が与えられたユーザよりのアクセスであると判断した場合に上記限定コンテンツをアクセスするアクセス手段を上記サーバ上のサービスディレクトリに設けたことにより、該限定コンテンツへのアクセス許可が与えられていないユーザからのアクセスを確実に防止することができる。

【図面の簡単な説明】

【図１】本発明の適用されるネットワークの概念図である。

【図２】本発明の一実施例のブロック図である。

【図３】本発明の一実施例のフロー図である。

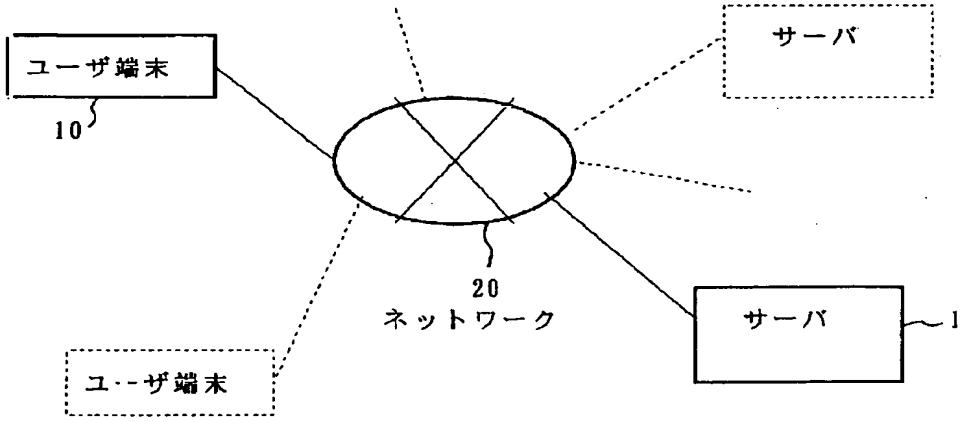
【図４】本発明の一実施例の画面例である。

【図５】従来のシステム概念図である。

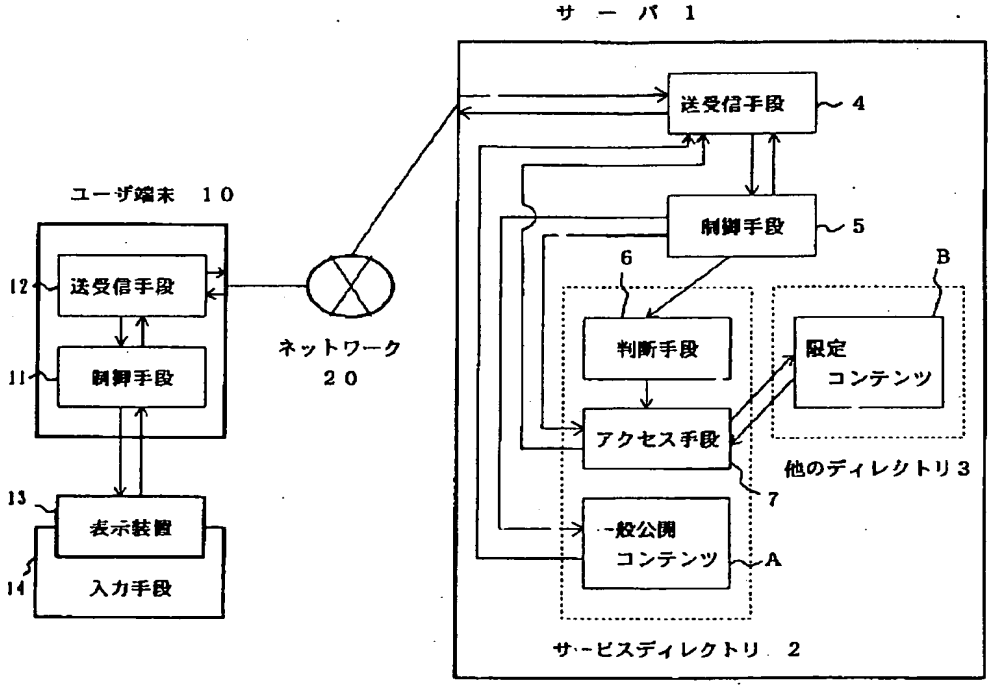
【符号の説明】

１、３１	サーバ
２　３２	サービスディレクトリ
３	他のディレクトリ
４、１２	送受信手段
５、１１	制御手段
６	パラメータ判断手段
７	アクセス手段
１０、３３	ユーザ端末
１３	表示装置
２０、３４	ネットワーク
Ａ	一般公開コンテンツ
Ｂ	限定コンテンツ

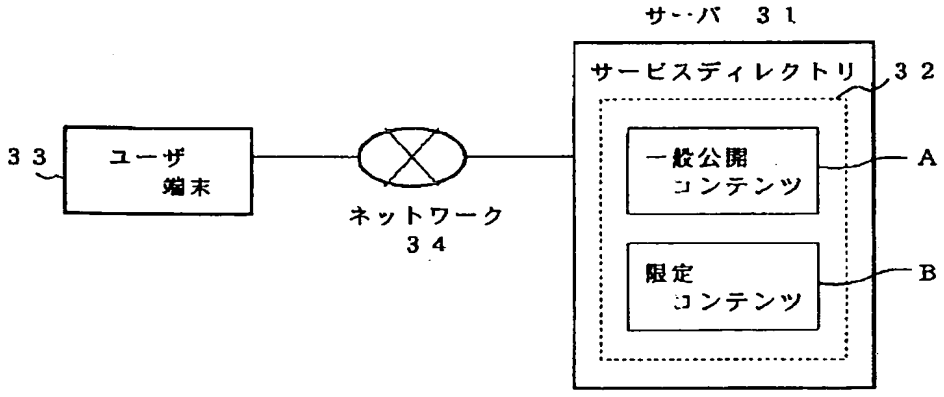
【図１】



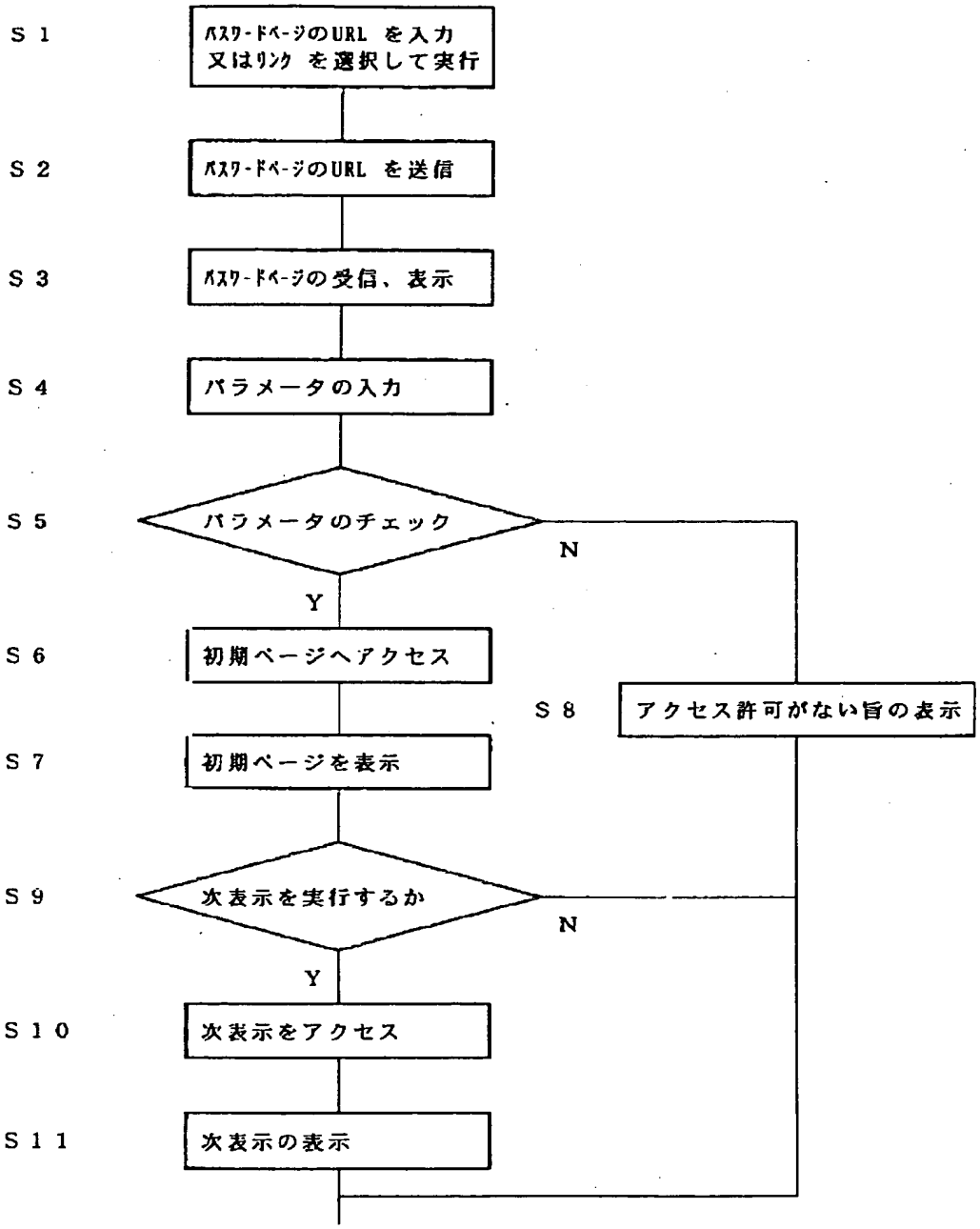
【図2】


サーバ 1
送受信手段
4
制御手段
5
6
B
判断手段
限定
コンテンツ
アクセス手段
他のディレクトリ3
7
一般公開
コンテンツ
A
サービスディレクトリ 2
ユーザ端末 10
12
送受信手段
11
制御手段
13
表示装置
14
入力手段
ネットワーク
20

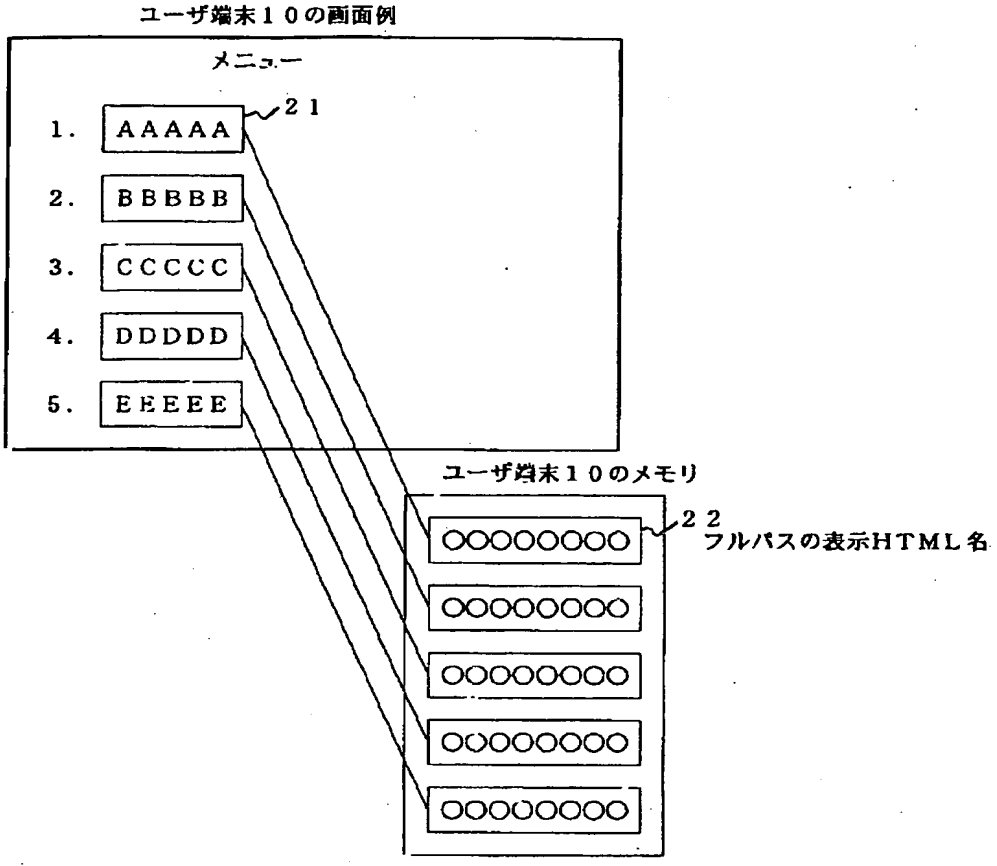
【図5】


サーバ 31
サービスディレクトリ
32
一般公開
コンテンツ
A
限定
コンテンツ
B
33
ユーザ
端末
ネットワーク
34

【図3】


S1
パスワードページのURL を入力
又はリンク を選択して実行
S2
パスワードページのURL を送信
S3
パスワードページの受信、表示
S4
パラメータの入力
S5
パラメータのチェック
N
Y
S6
初期ページへアクセス
S8
アクセス許可がない旨の表示
S7
初期ページを表示
S9
次表示を実行するか
N
Y
S10
次表示をアクセス
S11
次表示の表示

【図４】


ユーザ端末１０の画面例
メニュー
1. AAAAA
2. BBBBB
3. CCCCC
4. DDDDD
5. EEEEE
２１
ユーザ端末１０のメモリ
２２
フルパスの表示ＨＴＭＬ名